# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220713.19 | 13 июля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

## Множественные уязвимости в Motorola Solutions ACE1000

| | |
|---|---|
| Категория уязвимого продукта | Программно-аппаратное решение |
| Уязвимый продукт | ACE1000: Все версии |
| Дата выявления | 29 июня 2022 г. |
| Дата обновления | 29 июня 2022 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|---|---|---|
| MITRE: CVE-2022-30271 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена использованием жестко закодированного закрытого ключа SSH.<br>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C<br>CWE-321: Использование жестко закодированного ключа шифрования<br>Для исправления вручную смените закрытый ключ, используя процесс «Смена ключа SSH ACE1000». | 9.8 |

| | | |
|---|---|---|
| MITRE: CVE-2022-30270 | Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена использованием жестко закодированных данных.<br>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C<br>CWE-798: Использование жестко закодированных учетных данных<br>Для исправления пользователи должны изменить свой пароль вручную. Этот процесс можно найти в руководстве пользователя ACE1000. | 9.8 |
| MITRE: CVE-2022-30274 | Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена использованием жестко закодированного ключа.<br>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:U/RC:C<br>CWE-321: Использование жестко закодированного ключа шифрования<br>Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами | 7.5 |

| | |
|---|---|
| Ссылки на источники | http://ics-cert.us-cert.gov/advisories/icsa-22-179-06 |